OPM Data Breach:
What It Means To You

** Deckplate training for Navy Sailors **

What happened?

- On Thursday, 9 July, the Office of Personnel Management (OPM) announced a cyber incident exposed the **federal background investigation** data of current, former, and prospective federal employees, **military members**, and contractors.
- OPM provides Security Investigation services, including record retention, for the Department of Defense (DOD)
- The data of as many as 21.5 million background investigation applicants, spouses or co-habitants, and others may have been compromised.
- Background investigation (Standard Form (SF) 85, SF 85P, SF 86) data includes:
  - SSN
  - Residency & educational history
  - Employment history
  - Information about immediate family, personal & business acquaintances
  - Health (including mental health), criminal & financial history
- Compromised information may also include:
  - Interview notes taken by background investigators
  - Fingerprints

Am I affected?

- ☐ If you **entered the service** <u>since 2000</u>**, hold a current security clearance, or have had a background investigation** <u>since 2000</u>, you are affected

  - –Request could be for either a new investigation or periodic re-investigation

  - –Background investigations are requested by submitting Standard Form (SF) 85, 85P or 86 or by using the OPM electronic submission system

- ☐ Less likely but possible, if you submitted a request for a background investigation prior to 2000

Affected Individuals will be officially notified by Defense Manpower Data Center via U.S. Postal Service correspondence beginning in September

What are the risks?

- Data breaches involving personal information can result in a broad range of risks to military personnel including:
  - Identity theft
  - Targeting of individuals with knowledge of sensitive information
  - Intelligence activities that use personal information of U.S. citizens to undermine national security

- **Full scope of the risk is not fully known**

- If notified, it **does not** mean your identify will be stolen – but **YOU ARE AT RISK**

What is Navy doing?

☐ Due to the scope of the OPM data breach, Navy cannot act independently

☐ Response actions are being coordinated across the entire DOD

☐ Upon official notification military members will be entitled to **3-years of No Cost Identify Theft Protection Services**

  - $ 1 million dollars of identity theft insurance
    ▪ Retroactive to date of OPM data breach
  - Full service identify restoration support and victim recovery assistance
  - Continuous credit monitoring
  - Fraud monitoring services beyond credit files
  - Identity monitoring for minor children

☐ Official notifications will provide instructions for coverage enrollment

☐ Enrollment is not required for identity theft insurance coverage

  - Claims process not yet established, will be in place prior to notifications

What should I do?

❑ Enroll for **No Cost Identify Theft Protection Services** if you are officially notified that your information was compromised in the OPM breach

❑ Learn how to spot the warning signs of identity theft and protect yourself:

IdentityTheft.gov

- Get free credit reports
- Set up fraud alerts on your accounts
- Protect your children/minors from identify theft

❑ Ensure you are vigilant about your personal information
- Monitor your accounts
- Be aware of phishing scams
- Update account passwords frequently

❑ Beware of attempts to solicit personal and work related information
- If you are approached contact your commander, security manager, and NCIS

Where can I get more information?

❑ The Navy source of information is the SECNAVs OPM Breach website:

www.SECNAV.navy.mil/OPMbreachDON

- Content includes:
  - Regularly updated Frequently Asked Questions section containing latest information
  - Briefings for commanders and supervisors
  - ALNAV Messages related to the OPM Breach
  - Additional resources and information

❑ Defense Security Service Toolkit

http://pyi-toolkit.cdse.edu